# Department of Homeland Security Daily Open Source Infrastructure Report for 15 August 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

## Daily Highlights

- The Department of Homeland Security has lowered the transit threat alert level, so that operators of bus, train, subway, and passenger boat systems are permitted to relax security measures rushed into place after last month's deadly attacks. (See item 11)
- CNN reports New Mexico Governor Bill Richardson has declared a state of emergency in four counties along the Mexican border that have been "devastated" by crimes such as the smuggling of drugs and illegal immigrants. (See item 12)
- The Canadian Press reports electronic databases maintained by the Public Health Agency of Canada and the U.S. Centers for Disease Control and Prevention will be formally linked, allowing investigators in both countries to track rapidly and efficiently outbreaks of foodborne illness. (See item 19)



# Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 13, The Journal News (NY)* — **Nuclear security review ordered.** The Department of Homeland Security will lead a team of officials from five federal agencies into Indian Point nuclear power plant, located in Buchanan, NY, next month for a comprehensive security, part of a new program to strengthen the defense across 17 sectors of the nation's infrastructure. The

program has started with nuclear plants, agency officials said, because that sector is one of the most regulated, and it has a smaller roster of sites than other industries. "We look upon it as kind of an unprecedented coordinated effort by federal agencies in partnership with local and private sector folks to look at critical infrastructure and consider the potential consequences of an attack," said William Flynn, director of the agency's protective security division. "We'll also look at the response capability not only of the owner, but also the local law enforcement and the emergency response groups." Flynn said the Nuclear Regulatory Commission, the Federal Emergency Management Agency, the FBI, the Environmental Protection Agency, and the U.S. Coast Guard will send experts as part of the 10− to 12−person teams conducting the review.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20050813/NEWS02/508130325/1018

2. *August 12, Department of Energy* — **Second anniversary of Northeast blackout marked with progress.** Secretary of Energy Samuel W. Bodman on Friday, August 12, marked the second anniversary of the Northeast blackout during which 50 million Americans lost electricity by highlighting important progress that has been made to make North American electricity grids more reliable. On August 14, 2003, Americans throughout the Northeast lost electricity when problems at a utility in northern Ohio began a chain reaction of events that led to massive power outages. Since that time, the U.S. and Canadian governments, working with industry, have sought to ensure that all parties with responsibilities for grid management have the equipment and training needed to maintain safe, orderly operations under unusual or adverse conditions. Significant progress has been made, such as, enactment in the United States of the Energy Policy Act of 2005, which makes compliance by electric utilities and other companies with reliability standard mandatory and enforceable under federal law; establishment of an electric reliability division at the Federal Energy Regulatory Commission, which will advise the commission on standards proposed by industry−based organizations; and the North American Electric Reliability Council revised its existing reliability standards to clarify what constitutes compliance with them.
Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=18520&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

[Return to top]

## Chemical Industry and Hazardous Materials Sector

3. *August 12, The Indy Star (IN)* — **Tanker truck spill forces evacuation, road closure in Indiana.** A truck carrying nearly 7,000 gallons of flammable liquid overturned in Indiana and spilled part of its load, prompting officials to evacuate residents living within a half mile and to close a state highway for about 15 hours. The truck crashed Wednesday night, August 10, when it swerved to avoid an oncoming car on Indiana Route 32 a few miles east of Crawfordsville, IN, police said. The truck driver and two women in the car suffered minor injuries. "The tanker began leaking right away, and it was leaking...a gallon every 15 to 20 seconds," Montgomery County, IN, Sheriff's Deputy Luther Blanton said. The stretch of Indiana Route 32 was reopened Thursday morning, August 11, after the cleanup. The remaining fuel was transferred to another tanker.
Source: http://www.indystar.com/apps/pbcs.dll/article?AID=/20050812/ NEWS01/508120504

[Return to top]

## Defense Industrial Base Sector

Nothing to report.
[Return to top]

## Banking and Finance Sector

4. *August 12, Washington Post* — **Glitch on Verizon Wireless Website left data at risk.** Verizon Wireless said on Thursday, August 11, that computer programming flaws in its online billing system could have allowed customers to view account information belonging to other customers, possibly exposing limited personal information about millions of people. A spokesperson for the company declined to say how many of the company's 45 million subscriber accounts were at risk. Verizon Wireless said the problem appeared to be limited to accounts for customers in the eastern United States who had signed up for its "My Account" feature. There was no indication that anyone took advantage of the flaws or that any customer financial information, such as Social Security or credit card account numbers, was disclosed, Verizon Wireless spokesperson Tom Pica said. The flaws also did not allow access to phone numbers associated with customers' incoming and outgoing calls, and "no customer data could be manipulated and changed in any way," Pica said. Verizon Wireless said it had corrected the problem as of 2 a.m. Thursday.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/11/AR2005081102122.html

5. *August 12, The Register (UK)* — **New York enacts security breaches disclosure law.** New York has enacted an information security breaches law which will oblige firms and local government agencies to notify customers in the state if their personal information is taken or its systems are hacked. The legislation is designed to promote a culture of security. It also helps protect consumers by giving them the information they need to head off possible identity theft when sensitive details such as Social Security, driver's license and credit card numbers become exposed. Organizations with customers in New York are obliged to notify these people of a breach as soon as practically possible. The Information Security Breach and Notification Act in New York is broadly similar to security breaches laws enacted in California more than two years ago.
   Source: http://www.theregister.co.uk/2005/08/12/ny_security_breaches_disclosure/

6. *August 12, Los Angeles Times* — **New charges filed against identity thief.** Olatunji Oluwatosin, who pleaded no contest in February to one felony count of identity theft for his role in a fraud ring that stole data from ChoicePoint Inc., was charged last week in Los Angeles County Superior Court with six additional counts of identity theft, conspiracy and grand theft. Oluwatosin, a Nigerian national, remains the only person charged in the scheme, which exposed the Social Security numbers, addresses and other personal data of as many as 145,000 people to identity thieves. Documents filed under the new charges allege that Oluwatosin committed those crimes as part of a conspiracy with unnamed accomplices and caused at least

$2.5 million in damages. Armed with the ChoicePoint data, the conspirators opened credit card accounts in victims' names and then took out cash advances at automated teller machines, prosecutors alleged.
Source: http://www.latimes.com/business/la−fi−choicepoint12aug12,1,5993835.story?coll=la−headlines−business

7. *August 12, Banking Technology* — **German bank fights phishing with indexed transaction numbers.** Postbank has become the first major German bank to introduce indexed transaction numbers (iTANs) to fight online fraud. The bank has also extended the use of mobile transaction numbers for online banking in an attempt to protect its customers from phishing attacks. Customers could previously input any of the six digit transaction numbers from their hard copy list to guarantee their identity, however, with phishers increasingly trying to scam transaction numbers from customers, the bank decided to bring in the indexed numbers. Now customers have to enter a specified number for each online transaction they carry out so even if a scammer does manage to obtain a transaction number it will not work again. Similarly, if customers prefer, they can register for the mobile transaction numbers which are generated by online banking and sent to the customer via a text message. Again, the numbers are only valid for the requested transaction. Previously the mobile numbers could only be used with the retail portal Postbank direct.
Source: http://www.bankingtech.com/ipi/bankingtech/indextemplate.jsp?pageid=article&contentid=20017308314

8. *August 12, Dayton Business Journal (OH)* — **One−third of Ohio businesses ill prepared for blackout.** Sunday, August 14, marks the second anniversary of the worst energy blackout in U.S. history and a new study by AT&T finds that Ohio businesses have a long way to go before they could keep operating smoothly in a similar event. The blackout cost Ohio manufacturers more than $1 billion, but 32 percent of the Ohio businesses surveyed still lack business continuity plans and 40 percent do not see such planning as a priority. Business continuity plans consist of implementing safeguards and preparing for the unthinkable, according to the report. It highlights identifying and protecting critical processes and vital infrastructure as well as ensuring the stability of communication systems. The report also recommends that the plans are updated and tested every six months to reflect changes within the company. The report also recognizes that the threat of a digital meltdown is greater than natural disasters for many companies, and most Ohio businesses do include cybersecurity in their overall planning. However, 27 percent of those that do have continuity plans do not include cybersecurity.
Source:
More information about the report: http://www.att.com/news/2005/08/12−1

9. *August 09, WFAA−TV (TX)* — **Bank loses thousands of checks.** A truck carrying thousands of Federal Reserve Bank checks that were headed to Houston, TX, for sorting lost some of its cargo. The checks are already paid and canceled, but they have a combination of information that identity theft thieves could capitalize on, which include Social Security numbers, full names, addresses and signatures. The government clears millions of checks each week in Dallas for banks across Texas, half of New Mexico and Louisiana. Despite attempts to call during a weekend, there was no answer at the Federal Reserve number designated to notify if the lost items were found. However, after a television station alerted the reserve bank, they started an internal investigation and said they did not yet know how many checks may be lost. "We do

appreciate the good Samaritan who actually stopped and helped pick up the checks," said Diane Holloway, with the Federal Reserve Bank. She also said despite this incident, she believes the system is usually safe. "Accidents can happen," she said. "Human error can occur. But it is a very safe system and one that we take very seriously," said Holloway.
Source: http://www.wfaa.com/s/dws/news/localnews/tv/stories/wfaa050808_mo_checks.543a6b54.html

[Return to top]

## Transportation and Border Security Sector

10. *August 14, Associated Press* — **Pilots reportedly unconscious in plane crash north of Athens.** A Cypriot airliner crashed into a hill north of Athens on Sunday, August 14, killing all 121 people on board. Reports said at least one of the pilots was unconscious when the plane went down, possibly from lack of oxygen in the cabin. The Helios Airways flight HCY 522 was headed from Larnaca, Cyprus, to Athens International Airport when it crashed near the town of Grammatiko, about 25 miles north of the Greek capital, leaving flaming debris and luggage strewn across a ravine and surrounding hills. The Boeing 737, carrying 115 passengers and six crew, was to have flown onto Prague, Czech Republic, after stopping in Athens. Two F−16 fighter jets were sent out shortly after the plane entered Greek air space over the Aegean Sea and did not respond to radio calls −− a standard Greek practice. As they intercepted the airliner shortly before it crashed, the jet pilots saw one of the pilots slumped unconscious over the controls. Greek state television quoted Cyprus Transport Minister Haris Thrasou as saying the plane had decompression problems in the past. David Kaminski Morrow, deputy news editor of the British−based Air Transport Intelligence magazine, said depressurization is extremely serious because its effects happen so quickly.
Source: http://www.usatoday.com/news/world/2005−08−14−greece−crash_x .htm

11. *August 13, Washington Post* — **Terrorism alert level lowered for transit.** Department of Homeland Security Secretary Michael Chertoff lowered the threat level for the nation's mass transit and ferry systems on Friday, August 12, concluding a 36−day period of high alert after the train and bus bombings in London prompted fears of a copycat attack in the United States. Effective at 8 p.m. local time or after evening rush hours, state and local operators of bus, train, subway, and passenger boat systems were permitted to relax security measures rushed into place after last month's deadly attacks. In a written statement, Chertoff said that "there is no specific, credible intelligence information indicating that an attack in the United States is imminent." U.S. authorities raised the color−coded threat level from yellow, or elevated, to orange, or high, after four suicide bombers killed 52 people in London. The alert was extended after a failed bomb plot July 21 before returning to yellow yesterday. The attacks, along with last year's commuter rail blasts in Madrid, which killed 191 people, underscored the inherent vulnerability of public transit. U.S. authorities described the recent alert and ongoing efforts as an attempt to inject at least some unpredictability into the security profiles of open systems that transport 32 million people a day.
For more information see: http://www.dhs.gov/dhspublic/
Statement by Chertoff on lowering the threat level:
http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0718.xml
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08

/12/AR2005081200899.html

12. *August 13, CNN* — **Border emergency declared in New Mexico.** New Mexico Governor Bill Richardson declared a state of emergency Friday, August 12, in four counties along the Mexican border that he said have been "devastated" by crimes such as the smuggling of drugs and illegal immigrants. The declaration said the region "has been devastated by the ravages and terror of human smuggling, drug smuggling, kidnapping, murder, destruction of property and the death of livestock. ... "[It] is in an extreme state of disrepair and is inadequately funded or safeguarded to protect the lives and property of New Mexican citizens." New Mexico shares 180 miles of border with the Mexican state of Chihuahua. "The situation is out of hand," Richardson said Friday night on CNN, noting that one 54−mile stretch is particularly bad. The Mexican government issued a statement in which it acknowledged the problems along the border, but said it continues to make consistent efforts to target them along with U.S. authorities. Richardson's declaration makes $750,000 in state emergency funds available to Dona Ana, Luna, Grant and Hidalgo counties. According to Richardson's statement announcing the declaration, "Recent developments have convinced me this action is necessary −− including violence directed at law enforcement, damage to property and livestock, increased evidence of drug smuggling, and an increase in the number of undocumented immigrants."
Source: http://www.cnn.com/2005/US/08/12/newmexico/index.html

13. *August 13, Washington Post* — **Airline security changes planned.** The new head of the Transportation Security Administration (TSA) has called for a broad review of the nation's air security system to update the agency's approach to threats and reduce checkpoint hassles for passengers. Edmund S. "Kip" Hawley, an assistant secretary of homeland security, directed his staff to propose changes in how the agency screens two million passengers a day. The staff's first set of recommendations includes proposals to lift the ban on various carry−on items such as scissors, razor blades and knives less than five inches long. Also, if approved, only passengers who set off walk−through metal detectors or are flagged by a computer screening system will have to remove their shoes at security checkpoints. The proposal also would give screeners discretion in determining whether to pat down passengers. For example, screeners would not have to pat down "those persons whose outermost garments closely conform to the natural contour of the body." Some security analysts praised the agency's proposal, saying that security screeners spend too much time trying to find nail scissors and not enough time focused on today's biggest threat: a suicide bomber boarding an airplane. The TSA has very limited capability to detect explosives under a person's clothing, for example, and is trying to roll out more high−tech machines that can protect against such threats.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/12/AR2005081201557.html

14. *August 12, Associated Press* — **Staff returns to work after British Airways strike strands thousands.** British Airways (BA) said Friday, August 12, that all of its striking Heathrow Airport workers were returning to work after a 24−hour walkout that saw all flights canceled at the airport and about 70,000 travelers stranded. The airline said it would operate "a limited number of aircraft" starting at 8 p.m. London time. But it warned that the disruption caused by more than 500 canceled flights at one of the world's busiest airports would continue for many hours. About 1,000 baggage handlers and other ground staff walked out Thursday, August 11, in support of workers fired by catering firm Gate Gourmet. About 1,000 passengers spent the

night on floors and in seating areas at the airport, BA said, while about 4,000 had been put up in hotels nearby. Incoming flights were diverted to airports as far away as Newcastle in northern England and Glasgow, Scotland. Police with submachine guns patrolled the airport as usual. The Metropolitan Police said the strike had led to an escalation of security at Heathrow. There was a ripple effect around the world, as passengers due to fly to London found themselves stuck.
Source: http://www.usatoday.com/travel/news/2005−08−11−ba−strike_x.h tm

15. *August 11, GovExec* — **DHS plans Website to help identify transportation vulnerabilities.** The Department of Homeland Security (DHS) plans to set up a free Website that will allow owners and operators of transportation systems to voluntarily assess their security protections against terrorist attacks and receive recommendations on how to make improvements, the department announced this week. DHS is seeking public and industry comment on the Vulnerability Identification Self−Assessment Tool. The department submitted a request Wednesday, August 10, to the Office of Management and Budget for emergency processing and approval authority to move forward on developing the tool. Comments are due to OMB by September 9. If the tool is approved, owners or operators within the transportation sector would be able to voluntarily enter information about their security measures and risks into a Web interface at no charge. Transportation systems eligible include aviation, rail, pipelines, highways and bridges, and mass transit. The interface would request information concerning security countermeasures, such as plans, policies and procedures, training; access controls, physical security assets, security technologies and equipment, communications security, and information security. According to the notice, DHS estimates there are potentially three million respondents in the United States. Out of that, DHS predicts that about 300,000 −− or 10 percent −− might use the new tool.
Source: http://www.govexec.com/story_page.cfm?articleid=31980&dcn=to daysnews

[Return to top]

## Postal and Shipping Sector

16. *August 12, Fremont Tribune (NE)* — **Nebraska post office warns against counterfeit money orders.** Fremont Post Office officials are warning residents and banks about counterfeit money orders that have been circulating nationwide. Lori Doty, postal supervisor, said the counterfeit money orders were first passed in Fremont last fall and have sporadically appeared in the area. She said the fake money orders have mostly been used as payments for Internet purchases and the problem is ongoing. "We've sent notification to area banks," Doty said. "They have reference cards to check (authenticity)." She said residents also can easily identify counterfeit money orders. "There's a Ben Franklin watermark you can see when you hold them up to a light," Doty said. "There's also a security thread through the width of the money order to the left of the watermark that says 'USPS.'" In addition, U.S. Postal Service money orders are not available in amounts of more than $1,000. She said anything more than that amount is definitely fake.
Source: http://www.fremontneb.com/articles/2005/08/12/news/news6.txt

[Return to top]

# Agriculture Sector

17. *August 12, Stop Soybean Rust News* — **Rust in another three Florida counties, nine total this week.** Asian soybean rust was confirmed by testing Thursday, August 11, for three more Florida counties: Taylor, Columbia, and Hillsborough. That makes 18 Florida counties positive for rust, with half of those confirmations reported just this week. In Columbia County, which is bordered by rust−positive counties Hamilton and Alachua, the find was soybean from a sentinel plot. The rust was on kudzu in both Taylor County (north−central Florida on the coast) and Hillsborough County, which is the next county south from Pasco, the first county in the state to have rust this year. Santa Rosa, Okaloosa, and Holmes were confirmed Wednesday, August 10th and were all soybeans from soybean sentinel plots, and on Monday, August 8, Florida reported positive finds from the previous week in Alachua, Lee, and Hamilton counties.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=503

18. *August 12, Minnesota Ag Connection* — **Wheat disease decreases harvests in Minnesota.** An outbreak of a fungal grain disease is affecting wheat harvests in northwestern Minnesota −− decreasing at least one farmer's crop by almost half. It's the region's worst outbreak of fusarium head blight, commonly called scab, since 1997, said Marcia McMullen, a plant pathologist at North Dakota State University. The disease shrivels grain kernels and robs the crop of yield and quality. It also has infected wheat and barley fields in north−central North Dakota, where heavy rains plagued crop production, McMullen said. It's not clear how much the disease will cost the region's farmers, McMullen said.
Source: http://www.minnesotaagconnection.com/story−state.cfm?Id=700& yr=2005

[Return to top]

# Food Sector

19. *August 12, Canadian Press* — **Canada, U.S. health agencies to link database information.** Public health officials on both sides of the Canada−U.S. border will be able to trace outbreaks of foodborne pathogens such as E. coli with greater ease, thanks to an agreement signed Friday, August 12. Electronic databases maintained by the Public Health Agency (PHA) of Canada and the U.S. Centers for Disease Control and Prevention will be formally linked, allowing investigators in both countries to chase down more rapidly and efficiently outbreaks of foodborne illness that can be hard to spot because they occur over multiple states and provinces. "A lot of our food systems are very highly integrated. So what's happening in Canada can be happening in the U.S. and what's happening in the U.S. can be happening in Canada," Frank Plummer, scientific director of the PHA's National Microbiology Laboratory, explained.
Source: http://www.canoe.ca/NewsStand/LondonFreePress/News/2005/08/12/1169667−sun.html

[Return to top]

# Water Sector

**20.** *August 11, WMUR (NH)* — **Bacteria forces boil order in Peterborough.** A boil order has been issued for the town of Peterborough, NH, after dangerous bacteria was found in the town water supply. Health officials said tests revealed the presence of E. coli bacteria in samples of the town's water. Residents were told to boil their tap water for at least two minutes before drinking it. The bacteria can cause diarrhea, cramps, nausea, headaches and other symptoms. People with weakened immune systems are most at risk of becoming sick from drinking contaminated water. The source of the contamination was not known. Officials said they are chlorinating and flushing town wells and expect the problem to be resolved within two to three weeks.
Source: http://www.thewmurchannel.com/news/4838234/detail.html?subid=22101161&qs=1;bp=t

**21.** *August 11, San Francisco Chronicle (CA)* — **Audit says San Francisco water not secure.** The San Francisco, CA, Public Utilities Commission has been slow beefing up security along the Hetch Hetchy aqueduct to guard the regionally vital water system against terrorism, vandalism, and theft, according to an audit of the city−operated utilities. The report by Board of Supervisors Budget Analyst Harvey Rose's auditing team found that nearly four million dollars earmarked for security improvements had not been spent, and that plans to install electronic monitoring equipment had been moving slow. In addition, auditors voiced concern that the agency's emergency operations plans were not regularly updated. The audit also faulted the Public Utilities Commission for failing to fill the vacant security director position for more than a year.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/08/11/BAG4 AE66621.DTL

**22.** *August 10, U.S. Environmental Protection Agency* — **New tests to detect previously undetectable bacteria.** New test methods proposed Wednesday, August 10, by the U.S. Environmental Protection Agency (EPA) will lead to the detection of four types of bacteria in wastewater and sewage sludge. EPA's proposal centers on culture−based approaches to detecting enterococci and Escherichia coli (E. coli) in wastewater. Additional tests will identify salmonella and fecal coliform bacteria in sewage sludge. The bacteria are seen as "health indicators" that point to possible contamination and the need for further investigation and treatment. Until now, no EPA−approved tests were available to detect these bacteria in wastewater. The new tests will yield results within 24 hours and provide treatment facilities with an indication of the effectiveness of their treatment techniques.
Source: http://yosemite.epa.gov/opa/admpress.nsf/74de46851771ad928525702100565d7d/224e2614bf290faa8525705900644f15!OpenDocument

[Return to top]

## Public Health Sector

**23.** *August 12, Reuters* — **Second drug should be readied for bird flu.** A second influenza drug, GlaxoSmithKline's Relenza, should be stockpiled in readiness for a feared global pandemic of avian flu, researchers said on Thursday, August 11. The drug, known generically as zanamivir, is inhaled and some doctors have worried that patients may not be able to use it correctly, but the team of Asian doctors said it will be important to have as many antivirals on hand as possible. A dozen Asian nations agreed on Thursday, August 11, to build a regional stockpile of

drugs, mostly oseltamivir, made by Swiss pharmaceutical giant Roche under the brand name Tamiflu. Work is also underway to develop a vaccine to protect against H5N1. But this is not enough, argued Kenneth Tsang of the University of Hong Kong and colleagues. "Even if pharmaceutical manufacturing begins soon after an outbreak, there would not be a sufficient vaccine supply for the countries most in need − i.e., the Asian nations," they said. "Antiviral drugs are consequently the only specific treatment, pending availability of effective vaccines." Tsang and colleagues also called for clinical trials combining Relenza and Tamiflu to see if the combination works better than either drug alone.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2005−08−12T194247Z_01_MCC270883_RTRIDST_0_HEALTH−DRUG−BIRD−FLU−DC.XML

**24.** *August 12, Reuters* — **U.S. to require flu shots for nursing home patients.** U.S. nursing homes must vaccinate all their patients against the flu and pneumonia starting this fall or risk being kicked out of the Medicare and Medicaid programs under a new plan made public on Friday, August 12. The proposal, which has not yet been finalized, would ensure that the most vulnerable elderly receive their flu shots but could raise questions about how many doses will remain as Americans head into the 2005−2006 flu season with only two U.S.−approved vaccine makers. There are between 1.6 million and two million residents in approximately 18,000 nursing homes, according to various U.S. government estimates. Medicare officials said they came up with the nursing home rule after hearing from the U.S. Centers for Disease Control and Prevention and two industry groups −− the American Association of Homes and Services for the Aging and the American Health Care Association. Only 65 percent of nursing home residents received flu shots, according to one 1999 survey. Officials said they want to raise that figure to 90 percent. Nursing homes must also give pneumonia vaccine to patients who have never had it, officials said. Only 38 percent of elderly patients had received them, the 1999 survey found.
Source: http://today.reuters.com/business/newsArticle.aspx?type=health&storyID=nN12655034

**25.** *August 12, Reuters* — **Idaho probes outbreak of Creutzfeldt−Jakob disease.** Idaho officials said on Friday, August 12, an initial test has indicated one case of naturally occurring Creutzfeldt−Jakob disease (CJD) and they are investigating five other suspected cases. Tom Shanahan, a spokesperson for the Idaho Department of Health and Welfare, said five of the cases involve people who have already died, lived in neighboring counties and were over the age of 60. The sixth case centered on a man, also over the age of 60, who lived 90 miles away and was still alive. He said officials expected to receive the results of a more in−depth second test by the end of next week that would rule out any possibility the disease could be anything but the kind that occurs naturally. CJD is a rare brain−wasting disease in humans that usually affects older people in their 60s or 70s. It is not the same as the human form of mad cow disease, which is known as variant Creutzfeldt−Jakob Disease and is linked to eating beef from infected cattle. Naturally occurring CJD is found at a rate of about one case per one million population annually, according to the U.S. Centers for Disease Control. Yet in a state with only 1.4 million people the fact that Idaho has so many suspected cases of the rare disease has sparked concern.
Source: http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2005−08−12T215938Z_01_EIC265154_RTRIDST_0_USREP

ORT−IDAHO−DC.XML

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

**26.** *August 12, The Daily News (NC)* — **Emergency training goes to new heights in North Carolina.** Cell phone and communication towers are the newest focus for rescue workers in North Carolina trying to prepare themselves for as many potential situations as possible. "We want to be ready, efficient and effective," said Atlantic Beach, NC, Fire, Rescue and Emergency Medical Services Chief Adam Snyder. Snyder and members of the Atlantic Beach department were among the nearly 30 rescue workers from around North Carolina who spent last week in Carteret County participating in a tower−rescue training class that is the first of its kind in North Carolina. After one day in the classroom, the rescue workers headed to the site of a cell phone tower in Morehead City to put their skills to practice. On Thursday, August 11, participants used various devices and techniques for lowering victims to the ground. The goal was to prevent a person being lowered from hitting the structure. While training on the tower, class participants also learned about dealing with electrical, microwave, and other hazards. Source: http://www.jdnews.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=34155&Section=News

**27.** *August 11, Virginian−Pilot (VA)* — **North Carolina hospital completes disaster drill.** A disaster drill was held Wednesday, August 10, at Albemarle Hospital in Elizabeth City, NC, went quicker and smoother than previous drills have, emergency workers said. The scenario: A small airplane crashed near Elizabeth City; 40 people were dead and about a dozen survived, though many were doused with diesel fuel. Three fire engines, an ambulance, a Hazmat trailer, as well as public health and hospital staff assembled behind the hospital for the drill. About 20 hospital staffers played the role of injured victims and were told to cry and act like they were in pain, hospital spokesperson Chip Romanovich said. Albemarle Regional Health Services set up a temporary morgue, and a decontamination area was sealed to keep “fuel−soaked” victims from contaminating the rest of the hospital. The drill went quicker and more fluidly than the last major drill of its type, which was conducted last year, said Christy Saunders, emergency management coordinator for Pasquotank and Camden counties in North Carolina. The most important practice was on communication and coordination of all emergency services, Romanovich said. Though some things could have gone smoother, the lessons learned will help if a real disaster strikes, Elizabeth City Fire Chief William Pritchard said.
Source: http://home.hamptonroads.com/stories/story.cfm?story=90489&r an=12617

[Return to top]

## Information Technology and Telecommunications Sector

28. *August 12, US−CERT* — **Technical Cyber Security Alert TA05−224A: VERITAS Backup Exec Uses Hard−Coded Authentication Credentials.** VERITAS Backup Exec Remote Agent for Windows Servers is a data backup and recovery solution that supports the Network Data Management Protocol (NDMP). NDMP "...is an open standard protocol for enterprise−wide backup of heterogeneous network−attached storage." By default, the Remote Agent listens for NDMP traffic on port 10000/tcp. The VERITAS Backup Exec Remote agent uses hard−coded administrative authentication credentials. An attacker with knowledge of these credentials and access to the Remote Agent may be able to retrieve arbitrary files from a vulnerable system. The Remote Agent runs with SYSTEM privileges. Exploit code, including the credentials, is publicly available. US−CERT has also seen reports of increased scanning activity on port 10000/tcp. This increase may be caused by attempts to locate vulnerable systems. US−CERT recommends taking the following actions to reduce the chances of exploitation: * Use firewalls to limit connectivity so that only authorized backup server(s) can connect to the Remote Agent. The default port for this service is port 10000/tcp. * At a minimum, implement some basic protection at the network perimeter. When developing rules for network traffic filters, realize that individual installations may operate on non−standard ports. * In addition, changing the Remote Agent's default port from 10000/tcp may reduce the chances of exploitation. Please refer to VERITAS support document 255174 for instructions on how to change the default port.
Source: http://www.us−cert.gov/cas/techalerts/TA05−224A.html

29. *August 12, US−CERT* — **Exploit for vulnerability in Microsoft Plug and Play.** US−CERT is aware of a public exploit for a vulnerability in Microsoft Plug and Play that could allow an attacker to locally or remotely execute arbitrary code or cause a denial−of−service condition on a vulnerable system. The exploit code targets Windows systems by connecting to NetBIOS ports 139/tcp or 445/tcp on a vulnerable system. A remote, unauthenticated attacker may be able to execute arbitrary code or cause a denial−of−service condition on Windows 2000. With Windows XP SP1, the remote user must be authenticated to exploit the vulnerability. A local, authenticated attacker may be able to execute arbitrary code or to create a denial−of−service condition on Windows XP SP2 and Server 2003 systems. Microsoft has released a patch to address this vulnerability in Microsoft Security Bulletin MS05−039. Administrators are encouraged to apply the appropriate fixes as soon as possible.
VU#998653 − Microsoft Plug and Play contains a buffer overflow vulnerability:
http://www.kb.cert.org/vuls/id/998653
Patches from Microsoft: http://www.microsoft.com/technet/security/bulletin/ms05−aug. mspx
Source: http://www.us−cert.gov/current/current_activity.html#VU99865 3

30. *August 12, Novell* — **Buffer overflow vulnerability against eDirectory 8.7.3 imonitor on Windows.** There is a buffer overflow vulnerability against eDirectory 8.7.3 imonitor on Windows. This vulnerability will cause dhost.exe to crash causing a denial of service and can allow access to files. Users should apply edir873ptf_imon1.exe available at Novell Support Site to resolve the vulnerability. This fix should be applied to eDirectory 8.7.3 IR4 or 8.7.3 IR6. The fix will be included in IR7.
Source: http://support.novell.com/cgi−bin/search/searchtid.cgi?/1009 8568.htm

31. *August 11, Secunia* — **GNOME Evolution Multiple Format String Vulnerabilities.** Vulnerabilities have been reported in Evolution which can be exploited by malicious people to

compromise a vulnerable system. 1) A format string error when displaying full vCard information attached to an e−mail message can be exploited to execute arbitrary code. Successful exploitation requires that the user clicks on "Show Full vCard" or saves the vCard to an address book and then views it under the "Contacts" tab. 2) A format string error exists when displaying specially crafted contact data retrieved from an LDAP server. 3) A format string error exists when displaying specially crafted task list data retrieved from remote servers and when the user saves the task list data under the "Calendars" tab. The vulnerabilities have been reported in versions 1.5 through 2.3.6.1 and have reportedly been fixed in 2.3.7 (unstable).
Source: http://secunia.com/advisories/16394/

32. *August 11, Security Focus* — **McAfee ePolicy Orchestrator Local Information Disclosure Vulnerability .** Network Associates McAfee ePolicy Orchestrator is susceptible to a local information disclosure vulnerability. This issue is due to incorrectly configured directory permissions in the default installation process of the application. This vulnerability allows local attackers to access arbitrary files located in the same partition as the affected directory with SYSTEM privileges. This will aid them in further attacks. Security Focus is not currently aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/14549/references

## Internet Alert Dashboard

### DHS/US−CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** US−CERT is aware of a public exploit for a vulnerability in VERITAS Backup Exec Remote Agent for Windows Servers. This exploit may allow a remote attacker to retrieve arbitrary files on a system. The VERITAS Backup Exec Remote Agent listens on network port 10000/tcp. US−CERT is aware of reports that this vulnerability is being actively exploited. US−CERT has also seen reports of increased scanning activity on port 10000/tcp. This increase is believed to be attempts to locate vulnerable systems running the VERITAS Backup Exec Software. More information about this vulnerability can be found in US−CERT Technical Cyber Security Alert: TA05−224A − VERITAS Backup Exec Uses Hard−Coded Authentication Credentials. The following workarounds may mitigate this vulnerability: Restrict access to port 10000/tcp by using a firewall to limit access to the back−up service to only trusted entities. Change the default port for the backup service from port 10000/tcp to reduce the chances of exploitation

### Current Port Attacks

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (−−−), 445 (microsoft−ds), 6348 (−−−), 6881 (bittorrent), 1234 (hotline), 139 (netbios−ssn), 135 (epmap), 53 (domain), 1434 (ms−sql−m), 32772 (sometimes−rpc7)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

**33.** *August 13, Associated Press* — **Security cameras multiply in Manhattan.** Six surveillance cameras could be seen peering out from a chain drug store on Broadway. One protruded awkwardly from the awning of a fast−food restaurant. A supersized, domed version hovered like a flying saucer outside Columbia University. To the dismay of civil libertarians and with the approval of law enforcement, they've been multiplying at a dizzying rate all over Manhattan. New York City police detectives regularly rely on private security cameras in a bid to solve crimes. After makeshift grenades exploded outside the British consulate in midtown Manhattan on May 5, they studied scores of videotape and concluded that a still−unidentified cyclist likely tossed the devices before fleeing. The Metropolitan Transportation Authority plans to spend up to $250 million (euro200 million) to install new surveillance cameras in the city's vast subway system. The New York Police Department (NYPD) also has requested funding for about 400 digital video cameras to help combat robberies and burglaries in busy commercial districts. Police officers already watch live feeds from hundreds of cameras in city housing projects throughout the five boroughs, where "they are a proven deterrent," said NYPD spokesperson Paul Browne.
Source: http://news.yahoo.com/s/ap/20050813/ap_on_re_us/terror_eyes_on_the_city;_ylt=AmAT9mj.BlQW_XAYsOscJNxG2ocA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

# General Sector

**34.** *August 13, New York Times* — **New Hampshire towns lose tool against illegal immigrants.** A New Hampshire judge on Friday, August 12, threw out a novel strategy that two police departments had tried to use to combat illegal immigration. The strategy involved charging illegal immigrants with criminal trespassing, and in the last few months such citations were filed against at least nine people, most of them Mexicans, in the New Hampshire towns of New Ipswich and Hudson. The police chiefs of those towns had said they decided to take immigration matters into their own hands because overburdened federal immigration authorities were unable or unwilling to take action against immigrants who were not considered dangerous or otherwise a high law enforcement priority. Police departments from Florida to California considered taking similar steps if the charges were upheld in the New Hampshire courts. The Mexican government became concerned enough to pay some legal fees and to send its consul general in Boston to the court hearings. Judge, L. Phillips Runyon III of Jaffrey/Peterborough District Court, said the towns' actions could not be upheld because such immigration matters must be left to federal authorities. Runyon noted that local police departments that want to be involved in immigration enforcement must go through a training process that allows them to

become "deputies" of the Immigration and Customs Enforcement agency.
Source: http://www.nytimes.com/2005/08/13/national/13immig.html

[Return to top]

## DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

### DHS Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

### Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

### Department of Homeland Security Disclaimer